## Doctor Web anticipates increase in number of banking Trojan attacks on Android users

😻 news.drweb.com/show/

Doctor Web

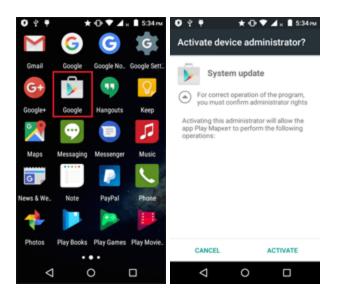


Back to news



Modern Android banking Trojans are created by virus writers and sold for serious sums as commercial products via underground Internet platforms. However, the source code of one such malicious application was recently made public on a hacker forum, along with instructions on how to use it. Doctor Web security researchers believe that this may lead to a significant increase in the number of attacks involving Android banking Trojans.

The virus writers published the source code of the new malicious application just one month ago, but Doctor Web security researchers have already detected an Android Banker that has been created using the information published by the cybercriminals. This Trojan, dubbed **Android.BankBot.149.origin**, is distributed under the guise of benign programs. When a smartphone or tablet user installs and runs **Android.BankBot.149.origin**, the banker prompts the user to grant it administrative privileges to hinder its removal from the system. After that it hides itself from the user by removing its shortcut from the home screen.



Then **<u>Android.BankBot.149.origin</u>** connects to the command and control (C&C) server and awaits instructions. The Trojan can execute the following actions:

- send SMS messages;
- intercept SMS messages;
- request administrator privileges;
- send USSD requests;
- obtain all contact list phone numbers;
- send SMS messages containing the text specified in a command to all contact list numbers;
- track device geolocation via GPS satellites;
- request additional permission on devices using the most recent Android versions to send SMS messages, make calls, and access the contact list and GPS receiver;
- receive an executable file containing a list of attacked banking applications;
- show phishing dialogs.

Like many other Android bankers, **Android.BankBot.149.origin** steals confidential user information by tracking the launch of online banking applications and payment system software. One sample examined by Doctor Web security researchers controls over three dozen such programs. Once **Android.BankBot.149.origin** detects that any of the aforementioned applications have been launched, it loads the relevant phishing input form to access user bank account login and password information and displays it on top of the attacked application.

<ul> <li></li></ul>	Войти в мой кошелек Введите номер телефона Пароль Войти
СБЕРБАНК выпустил онередной пакет важных и рекомендованных обновлений для своих банковских приложений. Для установки обновлений каки необходимо авторионроваться	Пароль
важных и рекомендованных обновлений для своих банковских приложений. Для установки обновлений кам необходимо авторионроваться	
авторионроваться	Войти
Авторизироваться	Войти
Bank of America ≫	PayPal
+380 Online ID	
Passcode	Usemame
ПН-код будь-якої вашої карти ПриватБанк.	Password
🔒 Авторизація	Continue

The Trojan not only steals mobile banking login credentials but also bank card information belonging to the owner of the compromised device. For this purpose,

<u>Android.BankBot.149.origin</u> tracks the launch of such popular applications as Facebook, Viber, Youtube, WhatsApp, Uber, Snapchat, WeChat, imo, Instagram, Twitter, and Play Store and displays a phishing dialog resembling the one used to make purchases on Google Play.

Soogle play	Enter your card details	Enter your card details		
Welcome to Google	YourBank	Forget something? Filp the card over.		
n connection with the change in the rules for use "Google Play", you				
need to register your bank card in our system	5105 1051 XXXX XXXX	000		
Registration takes less than two	YOUR NAME MANOCAND			
ninutes to proceed, click "Continue"				
Continue	Continue	Continue		

When an SMS message arrives, the Trojan turns off all sounds and vibrations, sends the message content to the cybercriminals, and attempts to delete the original messages from the list of incoming SMS. As a result, a user could miss not only bank notifications about the unplanned transactions but also other incoming messages.

<u>Android.BankBot.149.origin</u> uploads all the stolen data on the C&C server, and it becomes available on the administration panel. This helps cybercriminals to not only obtain the information they are interested in but also control the malicious application.

1223. 1223. 1225. 134.020 No. C181 Ratio L29 Ratio		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		NUMPLE           12117           201140208           12117           201140208           12131           201140208           2011           2010	N # 5 00 N # 5 00
SACCED     March2002     Samol 2.09     Samol		0 0 0 0 0		15:30 2011-01-06 2011-01-06 2015 2011-01-06 2015 2011-01-06 2017-01-06 2017-01-06 2017-01-07 2017-01-07 2017-01-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 15:52 2011-02-19 2012-02 20 20 20 20 20 20 20 20 20	NABO NABO NABO NABO NABO NABO
Interol.2019 Interol.2019 Intel Constant (Filewar) GT 20000 (GT 57000) GT 57000 Intelsion, Tabi Intelsion, Tabi Inte	- - - - - - - - - - - - - - - - - - -	0 0 0 0 0		2531 2011-01-08 29-05 29-05 29-05 29-14 29-05 29-14 29	
127 (2000) (277 (2000) (277 (2000) (277 (2000) (277 (2000) (277 (2000)) (277 (2000)) (277 (2000)) (277 (2000)) (277 (270 (277 (270 (270 (270 (270 (270		0 0 0 0 0		2011-01-00 29:05 29:05 20:15-01-00 29:05 20:17-01-00 29:17 20:17-01-00 29:17 20:17-01-10 29:06 20:17-01-10 29:06 20:17-01-10 29:07 20:15 20:15 20:17-01-10 29:07 20:17-01-10 29:07 20:17-01-10 29:07 20:17-01-10 29:07 20:17-01-10	
(T.A.1000) (G.J.SC2001) Rockaer Fab Backaer Fab Backaer Fab (T.A.400) (T.A.40		0 0 7 0 0		2017-01-06 20:35 20:35 20:37-02-09 20:37 20:37-02-09 20:37 20:37-02-19 20:37-02-19 20:52 20:37-02-19 20:52 20:37-02-19 20:52 20:37-02-19 20:52 20:37-02-19 20:52 20:37-02-19 20:52 20:37-02-09 20:52 20:55 20 20:55 20:55 20:5	
Instant Tak Borlant, Taki Borlant, Taki Borlant, Taki (21,66)		0 2 0 0	•	2831-82-09 26-33 2837-82-09 29-47 2847 2847 2847-82-19 16-12 2831-82-19 16 05 2837-82-19 2837-82-19	
04.20184 (273,688) (264,600) (196,620,02) (196,620,12,179) (196,620,12,179) (196,620,12,179) (196,620,128) (196,620,128) (196,620,128) (197,63,680) (177,630) (177,63	- - - - - - - - - - - - - - - - - - -	• • •	•	2011.01.09 29.47 2907-40-10 16:12 2011-02-10 18:08 2011.02.10	
345-4005 pro_colP() (1)(8)(5)(2)(2)(1)(9) (1)(8)(5)(2)(2)(1)(9) (1)(8)(5)(2)(1)(9) (1)(8)(2)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)(1)	(m)	0 0	•	29(11-00-10 16:12 29(11-00-10 18:08 29(11-00-10	
[URRCSLE_TSP (INTER)	(m)	0	•	2821-85-10 18 OK 2827.40.10	
27.29408 (a/3pp) 504.00.128 (2ama) (a) (24.001118 (2ama) (a) (21.2010 (27.2010) (27.2010) (27.2010) (27.40	* * *	0	•	2011-01-10	Date -
M-GUISE Land yea) M-GUISE paniptimerrige TT-SMRE GT-SORO GT-SORO LIT-BIODI LIT-BIODI DISTORTATION	* * *	•	-	18:42	NAB 0
MA-GOTTR (pandprimer effpe 07-55890) 07-56890 07-56890 07-86800 07-86800 07-9742 09-699940	(m) •	-		2907-80-89	NAB 0
CT.33440 CT.539300 CT.539300 CT.539300 CT.539300 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.539000 CT.5390000 CT.5390000 CT.539000 CT.53900000000 CT.53900000000000000000000	(m) •	- P	_	21(1)-0(2-10)	
GT-Solesty GT-Solesty GT-Solesty GT-Sitest Delegendered	-	-	-	20-13	110
pro associo o norice di Delegendento		•	-	16/31 29/11-80-13	NEB (B)
(teleprolog)	×	•	•	07.06	1.8
NALESON P.	*	•	•	2811-85-13 87,07	N# [6]
(cSgo)	×	۰	•	2011-00-13	N # 🕒 🙆
GT-6557WE EXT-800 TOED	×	•	•	2901-40-13 82.67	1200
UT-56107	*		•	2011-01-13	NA 📐 🚇
CT-838300. (CT-5383000	*	•	•	2811-40-13	NR
M-GUIN		*	•	2911-40-12 82-67	11.0
CNOC Past	*	•	•	2011-03-13	NA DO
		•	•	2911-40-1D	110
			•	2011-02-13	NA DO
SALESHIEL	~		-	2011-00-15	NA DO
	-	-	-	2017-00-12	1100
(Clyss)				02.11	AT DO MO
(Class) M. Class (Class) M. John (Class)	H	4 <b>*</b> 11 <b>*</b>			4 000 31-80-15 2100 4 00 1100 1000 1

In general, the possibilities of this Trojan are quite standard for modern Android bankers. However, as cybercriminals created it with publicly available information, one can anticipate that many Trojans similar to it will appear. Dr.Web for Android successfully detects <u>Android.BankBot.149.origin</u>; therefore, this malicious program poses no threat to our users.

More about this Trojan

## Protect your Android device with Dr.Web now

Buy online Buy on Google Play Free download

What is the benefit of having an account?

## Tell us what you think

To ask Doctor Web's site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

## Other comments

